

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

---

IN RE LAFAYETTE FEDERAL CREDIT  
UNION DATA BREACH LITIGATION

Case No. 8:25-cv-01006-DLB  
(Consolidated)

This Document Relates to: All Actions

---

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO  
DISMISS PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT**

**TABLE OF CONTENTS**

	<b>Page</b>
INTRODUCTION .....	1
BACKGROUND .....	2
ARGUMENT .....	3
I. Standard of Review .....	3
II. Plaintiffs Fail to Allege Facts Demonstrating Article III Standing .....	4
A. Plaintiffs Have Not Suffered an Article III Injury .....	6
1. Risk of Identity Theft and Fraud .....	7
2. Mitigation Efforts .....	12
3. Emotional Harms .....	12
4. “Theft” of PII .....	13
5. Diminution of Value of Personal Information .....	13
6. Invasion of Privacy .....	15
7. Loss of Benefit of the Bargain .....	17
B. Plaintiffs Fail to Allege an Injury Traceable to Lafayette .....	18
C. California Plaintiffs Darbinyan and Lewis Lack UCL Standing .....	20
III. Plaintiffs Fail to State a Claim .....	20
A. Plaintiffs’ Negligence (Count I) and Negligence Per Se (Count IV) Claims Should Be Dismissed .....	21
1. Lafayette Owed No Duty of Care Because There is No Contractual Privity .....	23
2. There is No Evidence of Negligence Based on Statutory Violation .....	23
3. There is No Duty of Care Based on an Indirect Special Relationship .....	24
4. No Duty Exists Based on the Actions of a Third Party .....	26

B. Plaintiffs’ Breach of Implied Contract Claim (Count II) Should Be Dismissed .. 27

C. Plaintiffs’ Unjust Enrichment Claim (Count III) Should Be Dismissed..... 30

D. Plaintiffs’ Breach of Fiduciary Duty Claim (Count V) Should Be Dismissed ..... 32

E. Plaintiffs’ Invasion of Privacy Claim (Count VI) Should Be Dismissed ..... 34

F. Plaintiffs Fail to State a Claim Under California Law..... 35

1. Plaintiffs Fail to Plausibly Allege that California Law Applies ..... 35

2. Plaintiffs Fail to State a Claim Under the UCL (Count VII) ..... 36

3. Plaintiffs Fail to State a Claim Under the CCPA (Count VIII) ..... 37

CONCLUSION..... 38

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Absolon v. Dollahite</i> , 376 Md. 547 (2003) .....	21
<i>Adcor Indus., Inc. v. Beretta U.S.A. Corp.</i> , 250 Md. App. 135 (2021) .....	30
<i>Ali v. Hogan</i> , 26 F.4th 587 (4th Cir. 2022) .....	3
<i>Alig v. Shea</i> , 126 F.4th 965 (4th Cir. 2025) .....	5, 11
<i>Alvarez v. Becerra</i> , No. 21-2317, 2023 WL 2908819 (4th Cir. Apr. 12, 2023) .....	5
<i>Ashburn v. Anne Arundel Cnty.</i> , 306 Md. 617 (1986) .....	24
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	3, 18
<i>Aton Ctr., Inc. v. CareFirst of Md., Inc.</i> , No. CV DKC 20-3170, 2021 WL 1856622 (D. Md. May 10, 2021) .....	35
<i>Baehr v. Creig Northrop Team, P.C.</i> , 953 F.3d 244 (4th Cir. 2020) .....	4
<i>Bailer v. Erie Ins. Exch.</i> , 344 Md. 515 (1997) .....	34
<i>Bank of Am. Corp. v. Gibbons</i> , 173 Md. App. 261 (2007) .....	31
<i>Basconcello v. Experian Info. Sols., Inc.</i> , No. 16-cv-06307-PJH, 2017 WL 1046969 (N.D. Cal. Mar. 20, 2017) .....	14
<i>Beck v. McDonald</i> , 848 F.3d 262 (4th Cir. 2017) .....	<i>passim</i>
<i>Bednyak v. Fin. Risk Mitigation, Inc.</i> , 739 F. Supp. 3d 353 (E.D. La. 2024) .....	15

<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	3
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997).....	5
<i>Berry &amp; Gould, P.A. v. Berry</i> , 360 Md. 142 (2000) .....	30
<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009) .....	20
<i>Blackman v. Ne. Spine &amp; Sports Med., LLC</i> , No. 24-7022 (ZNQ), 2025 WL 77029 (D.N.J. Jan. 13, 2025).....	28
<i>Braude v. Robb</i> , 255 Md. App. 383 (2022) .....	28, 29
<i>Brault Graham, LLC v. Law Offices of Peter G. Angelos, P.C.</i> , 211 Md. App. 638 (2013) .....	28
<i>Brooks v. Peoples Bank</i> , 732 F. Supp. 3d 765 (S.D. Ohio 2024) .....	31, 33
<i>Burger v. Healthcare Mgmt. Sols., LLC</i> , No. RDB-23-1215, 2024 WL 473735 (D. Md. Feb. 7, 2024) .....	<i>passim</i>
<i>Chalmers v. Toyota Motor Sales, USA, Inc.</i> , 935 S.W.2d 258 (Ark. 1996).....	35
<i>Chambliss v. Carefirst, Inc.</i> , 189 F. Supp. 3d 564 (D. Md. 2016) .....	18
<i>Chang-Williams v. Dep’t of the Navy</i> , 766 F. Supp. 2d 604 (D. Md. 2011).....	26
<i>Chernick v. Chernick</i> , 327 Md. 470 (1992) .....	29
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1974).....	6, 11
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	<i>passim</i>
<i>Cravens v. Garda CL Se., Inc.</i> , No. 24-CV-80400-RLR, 2024 WL 5058304 (S.D. Fla. Dec. 6, 2024).....	33

<i>Decoster v. Becerra</i> , 119 F.4th 332 (4th Cir. 2024) .....	2
<i>Disability Rights S.C. v. McMaster</i> , 24 F.4th 893 (4th Cir. 2022) .....	16
<i>Dolan v. McQuaide</i> , 215 Md. App. 24 (2013) .....	27, 28
<i>E.I. du Pont de Nemours &amp; Co. v. Kolon Indus.</i> , 637 F.3d 435 (4th Cir. 2011) .....	2
<i>Eastland Food Corp. v. Mekhaya</i> , 486 Md. 1 (2023) .....	30
<i>Erie Ins. Exch. v. Heffernan</i> , 399 Md. 598 (2007) .....	21
<i>Erie R.R. v. Tompkins</i> , 304 U.S. 64 (1938) .....	21
<i>Exxon Shipping Co. v. Baker</i> , 554 U.S. 471 (2008) .....	23
<i>FDA v. All. for Hippocratic Med.</i> , 602 U.S. 367 (2024) .....	5
<i>Fontenberry v. MV Transp., Inc.</i> , 984 F. Supp. 2d 1062 (E.D. Cal. 2013) .....	35
<i>Francis v. Giacomelli</i> , 588 F.3d 186 (4th Cir. 2009) .....	3
<i>Friends for Ferrell Parkway v. Stasko</i> , 282 F.3d 315 (4th Cir. 2002) .....	5
<i>Froelich v. Erickson</i> , 96 F. Supp. 2d 507 (D. Md. 2000) .....	32
<i>Furman v. Sheppard</i> , 130 Md. App. 67 (2000) .....	34
<i>Giasson v. MRA - Mgmt. Ass’n, Inc.</i> , No. 24-CV-839-JPS-JPS, 2025 WL 1025173 (E.D. Wis. Apr. 7, 2025) .....	33
<i>Gordon v. Zeroed-In Tech., LLC</i> , No. 23-3284-BAH, 2025 WL 936415 (D. Md. Mar. 26, 2025) .....	35, 36

<i>Griffey v. Magellan Health Inc.</i> , 562 F. Supp. 3d 34 (D. Ariz. 2021) .....	37, 38
<i>Harper v. Trans Union, LLC</i> , No. DKC 24-230, 2025 WL 1928021 (D. Md. July 14, 2025) .....	22
<i>Harvey v. Nat’l Amusements, Inc.</i> , No. 24-10027-GAO, 2025 WL 928776 (D. Mass. Mar. 17, 2025) .....	32
<i>Hill v. Workday, Inc.</i> , 773 F. Supp. 3d 779 (N.D. Cal. 2025) .....	36
<i>Hoffman v. Stamper</i> , 385 Md. 1 (2005) .....	13
<i>Holland v. Consol Energy, Inc.</i> , 781 F. App’x 209 (4th Cir. 2019) .....	7
<i>Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.</i> , 892 F.3d 613 (4th Cir. 2018) .....	<i>passim</i>
<i>Huynh v. Quora, Inc.</i> , 508 F. Supp. 3d 633 (N.D. Cal. 2020) .....	20
<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011), <i>aff’d</i> , 572 F. App’x 494 (9th Cir. 2014) .....	20
<i>In re Gallagher Data Breach Litig.</i> , 631 F. Supp. 3d 573 (N.D. Ill. 2022) .....	31
<i>In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig.</i> , No. 19-md-2879, 2020 WL 6290670 (D. Md. Oct. 27, 2020) .....	22, 25, 26
<i>In re NCB Mgmt. Servs., Inc. Data Breach Litig.</i> , 748 F. Supp. 3d 262 (E.D. Pa. 2024) .....	31
<i>In re Sabin Oral Polio Vaccine Prod. Liab. Litig.</i> , 774 F. Supp. 952 (D. Md. 1991), <i>aff’d</i> , 984 F.2d 124 (4th Cir. 1993) .....	21
<i>In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.</i> , 45 F. Supp. 3d 14 (D.D.C. 2014) .....	17
<i>Int’l Equip. Trading v. Illumina, Inc.</i> , 312 F. Supp. 3d 725 (N.D. Ill. 2018) .....	35
<i>J.R. v. Walgreens Boots All., Inc.</i> , No. 20-1767, 2021 WL 4859603 (4th Cir. Oct. 19, 2021) .....	22

<i>Jackson v. 2109 Brandywine, LLC</i> , 180 Md. App. 535 (2008) .....	31
<i>Jacques v. 1st Nat’l Bank</i> , 307 Md. 527 (1986) .....	23
<i>Jones v. Specialized Loan Servicing</i> , No. RDB-22-1987, 2023 WL 1442435 (D. Md. Feb. 1, 2023) .....	23
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009) .....	36
<i>Kiriakos v. Phillips</i> , 448 Md. 440 (2016) .....	24
<i>Kuechler v. Peoples Bank</i> , 602 F. Supp. 2d 625 (D. Md. 2009) .....	33
<i>Kuhns v. Scottrade, Inc.</i> , 868 F.3d 711 (8th Cir. 2017) .....	29
<i>Lebron v. Rumsfeld</i> , 670 F.3d 540 (4th Cir. 2012) .....	11
<i>Lloyd v. Gen. Motors Corp.</i> , 397 Md. 108 (2007) .....	22
<i>Lugo v. Inova Health Care Servs.</i> , No. 1:24-cv-700, 2025 WL 905191 (E.D. Va. Mar. 25, 2025).....	32
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	5
<i>Lyon v. Campbell</i> , 120 Md. App. 412 (1998) .....	11, 32
<i>Maag v. U.S. Bank, Nat’l Ass’n</i> , No. 21-0031, 2021 WL 5605278 (S.D. Cal. Apr. 8, 2021).....	38
<i>Mass Transit Admin. v. Granite Constr. Co.</i> , 57 Md. App. 766 (1984) .....	27
<i>Mgaresh v. Va. Union Univ.</i> , No. 3:24-cv-337-HEH, 2025 WL 641432 (E.D. Va. Feb. 27, 2025).....	34
<i>Mitchell v. Balt. Sun Co.</i> , 164 Md. App. 497 (2005) .....	34



<i>Mitchell v. WSG Bay Hills IV, LLC</i> , No. RDB–12–2036, 2013 WL 6502875 (D. Md. Dec. 11, 2013).....	25, 27
<i>Mogavero v. Silverstein</i> , 142 Md. App. 259 (2002) .....	27, 30
<i>Oman v. Delta Air Lines, Inc.</i> , 889 F.3d 1075 (9th Cir. 2018) .....	35
<i>Parker v. Columbia Bank</i> , 91 Md. App. 346 (1992) .....	32, 33
<i>Patton v. U.S. of Am. Rugby Football</i> , 381 Md. 627 (2004) .....	22, 25
<i>Paul v. Blackburn Ltd. P'ship</i> , 211 Md. App. 52 (2013), <i>aff'd</i> , 438 Md. 100 (2014) .....	21
<i>Plank v. Cherneski</i> , 469 Md. 548 (2020) .....	32
<i>Podroykin v. Am. Armed Forces Mut. Aid Ass'n</i> , 634 F. Supp. 3d 265 (E.D. Va. 2022) .....	9, 10, 13, 14
<i>Polek v. J.P. Morgan Chase Bank, N.A.</i> , 424 Md. 333 (2012) .....	33
<i>Pruchnicki v. Envision Healthcare Corp.</i> , 845 F. App'x 613 (9th Cir. 2021) .....	14
<i>Remsburg v. Montgomery</i> , 376 Md. 568 (2003) .....	24, 25, 27
<i>Ruiz v. Gap Inc.</i> , No. 07-5739 SC, 2009 WL 250481 (N.D. Cal. Feb. 3, 2009), <i>aff'd</i> , 380 F. App'x 689 (9th Cir. 2010) .....	20
<i>Russ v. Barnes</i> , 23 Md. App. 691 (1974) .....	29
<i>Spaulding v. Wells Fargo Bank, N.A.</i> , 714 F.3d 769 (4th Cir. 2013) .....	23, 32
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016).....	3, 4, 5
<i>Stamat v. Grandizio Wilkins Little &amp; Matthews, LLP</i> , No. SAG-22-00747, 2022 WL 3919685 (D. Md. Aug. 31, 2022).....	12

<i>State Constr. Corp. v. Slone Assocs., Inc.</i> , 385 F. Supp. 3d 449 (D. Md. 2019) .....	29
<i>Stratton v. Mecklenburg Cnty. Dep’t of Soc. Servs.</i> , 521 F. App’x 278 (4th Cir. 2013) .....	4
<i>Stuart v. Kyocera AVX Components Corp.</i> , 769 F. Supp. 475 (D.S.C. 2025).....	<i>passim</i>
<i>Susan B. Anthony List v. Driehaus</i> , 573 U.S. 149 (2014).....	4, 11
<i>TransUnion LLC v. Ramirez</i> , 594 U.S. 413 (2021).....	5, 13, 16
<i>United States ex rel. Carson v. Manor Care, Inc.</i> , 851 F.3d 293 (4th Cir. 2017) .....	38
<i>United States v. Texas</i> , 599 U.S. 670 (2023).....	4
<i>Vance v. Vance</i> , 286 Md. 490 (1979) .....	13
<i>Veney v. Wyche</i> , 293 F.3d 726 (4th Cir. 2002) .....	4
<i>Volvo Trademark Holding v. AIS Const. Equip. Corp.</i> , 416 F. Supp. 2d 404 (W.D.N.C. 2006) .....	35
<i>Warr v. JMGM Grp., LLC</i> , 433 Md. 170 (2013) .....	26
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	3
<i>Webb v. Injured Workers Pharmacy, LLC</i> , No. 22-CV-10797, 2023 WL 5938606 (D. Mass. Sept. 12, 2023) .....	32
<i>Welborn v. IRS</i> , 218 F. Supp. 3d 64 (D.D.C. 2016).....	14
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990).....	4, 10
<i>Yousef v. Trustbank Sav., F.S.B.</i> , 81 Md. App. 527 (1990) .....	33

<i>Zlotnick v. Equifax Info. Servs., LLC</i> , 583 F. Supp. 3d 387 (E.D.N.Y. 2022) .....	14
---	----

## **Statutes**

Cal. Civ. Code § 1798.145(a)(7).....	37
Cal. Civ. Code § 1798.150(a)(1).....	37
California Unfair Competition Law (“UCL”).....	<i>passim</i>
Consumer Privacy Act (“CCPA”) .....	<i>passim</i>
Federal Trade Commission Act (the “FTC Act”) .....	21, 22, 24
Gramm-Leach-Bliley Act (“GLBA”) .....	21, 22, 24

## **Other Authorities**

Fed. R. Civ. P. 10(c) .....	2
Fed. R. Civ. P. 12(b)(1).....	3
LAFAYETTE FEDERAL CREDIT UNION, <a href="https://www.lfcu.org/impact-about/lafayette-federal">https://www.lfcu.org/impact-about/lafayette-federal</a> .....	2
Restatement (Second) of Torts § 652A(2): (a) .....	34
Rule 9(b) .....	36
Rule 12(b)(6).....	3
U.S. Const. art. III.....	<i>passim</i>

Defendant Lafayette Federal Credit Union (“**Lafayette**”) submits this Memorandum of Law in Support of its Motion to Dismiss Plaintiffs’ Consolidated Class Action Complaint (the “**Complaint**” or “**Compl.**,” ECF No. 23).

### **INTRODUCTION**

This putative class action arises from a data security incident in which unauthorized actors gained access to a single employee email account maintained by Lafayette. Upon discovering the breach, Lafayette immediately secured the account, retained a forensic investigation firm, and confirmed that its broader systems were not compromised so that it could promptly notify those affected. Almost a year has gone by and Lafayette has no evidence of any actual or attempted misuse of the data. Nonetheless, Plaintiffs bring this suit based on a series of conjectural injuries: the perceived risk of identity theft, diminution in value of their personal information, invasion of privacy, loss of benefit of the bargain, lost opportunity, fear and stress, and annoyance and inconvenience, among others. They assert eight causes of action, including negligence and negligence *per se*, unjust enrichment, breach of implied contract, breach of fiduciary duty, invasion of privacy, and alleged violations of California’s Unfair Competition Law (“**UCL**”) and Consumer Privacy Act (“**CCPA**”).

The Complaint should be dismissed in full. First, Plaintiffs lack Article III standing. Courts routinely reject lawsuits premised on speculative and attenuated harms—particularly where, as here, there is no allegation of actual misuse of the data. Second, each of Plaintiffs’ claims independently fails on the merits. Lafayette owed no legal duty under Maryland law that would support Plaintiffs’ negligence or fiduciary duty theories. No enforceable agreement exists to support a claim for breach of implied contract, nor is there any basis for unjust enrichment. The alleged privacy invasion is unsupported and duplicative of Plaintiffs’ other claims, and their statutory claims under CCPA and UCL collapse with their failure to plead any cognizable

economic injury. Plaintiffs’ allegations, in short, cannot support the sweeping relief they seek.

### **BACKGROUND<sup>1</sup>**

Lafayette is a not-for-profit, financial institution, operating ten full-service branch locations in the District of Columbia, Maryland, and Virginia. Compl. ¶ 130.<sup>2</sup> Rooted in the region since 1935, Lafayette is a trusted partner focused on empowering its members with partnership-minded financial services. LAFAYETTE FEDERAL CREDIT UNION, <https://www.lfcu.org/impact-about/lafayette-federal>. To protect member data, Lafayette “use[s] security measures that comply with federal law,” including “computer safeguards and secured files and buildings” and maintains “physical, electronic, and procedural safeguards.” *See* Compl. ¶ 129 n.2 (citing Lafayette’s Privacy Policy).

On September 16, 2024, Lafayette identified unauthorized access to a single employee email account. *See id.* ¶ 132, Exs. 1–2. Lafayette responded promptly—securing the account, initiating an internal investigation, and engaging a third-party forensic firm to assess the incident. *See id.* The investigation determined that the account was accessed for a brief period and may have contained personal information, such as names and account numbers. *See id.* Despite having “no reason to believe that [any] personal information ha[d] been misused for the purpose of committing fraud or identity theft,” Lafayette notified members that the threat actor “may have acquired the

---

<sup>1</sup> The facts in this section are accepted as true solely for purposes of this motion. *See infra* Standard of Review. The “Notice of Data Security Incident,” attached to the Complaint as Exhibits 1–2, and the privacy policy cited as n.2 of Plaintiffs’ Complaint are considered “part of the pleading.” Fed. R. Civ. P. 10(c); *see also E.I. du Pont de Nemours & Co. v. Kolon Indus.*, 637 F.3d 435, 448 (4th Cir. 2011) (“In deciding whether a complaint will survive a motion to dismiss, a court evaluates the complaint in its entirety, as well as documents attached or incorporated into the complaint.”). They are also integral to the Complaint and authentic, as Plaintiffs rely heavily on the truth of their contents. *See Decoster v. Becerra*, 119 F.4th 332, 336 n.1 (4th Cir. 2024) (a document is “integral to the complaint” where the complaint “specifically references” it).

<sup>2</sup> Although alleged to be a for-profit corporation with eight full-service branch locations, Lafayette is, in fact, a not-for-profit financial institution with ten branch locations, as reflected on its website referenced and incorporated by the Complaint. *Compare* Compl. ¶¶ 130, 297, with <https://www.lfcu.org/locations-atms/> (last accessed July 31, 2025).

information contained in the account.” *See id.*, Exs. 1–2. Lafayette also advised members on how to monitor and protect their information and provided one year of Experian Identity Works<sup>sm</sup> Credit 3B, a credit monitoring and identity protection service. *See id.*

Seven individuals who received those notices now bring this putative class action. Although it has been over ten months since the data security incident, and there are no allegations of identity theft or fraud, Plaintiffs seek over \$5,000,000 in damages, as well as declaratory and injunctive relief.

## **ARGUMENT**

### **I. Standard of Review**

Lafayette moves to dismiss the Complaint under Federal Rule of Civil Procedure 12(b)(1) for lack of subject-matter jurisdiction. *See Ali v. Hogan*, 26 F.4th 587, 595 (4th Cir. 2022) (dismissal “for want of Article III standing” is a dismissal for “lack of subject-matter jurisdiction” under Rule 12(b)(1)). At the pleadings stage, the “plaintiff must ‘clearly . . . allege facts demonstrating’” each element of standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)). Conclusory allegations do not suffice. *Beck v. McDonald*, 848 F.3d 262, 270 (4th Cir. 2017). Only “allegations for which there is sufficient ‘factual matter’ to render them ‘plausible on [their] face’” are “accept[ed] as true.” *Id.*

Lafayette also moves to dismiss the Complaint under Rule 12(b)(6) for failure to state a claim. To withstand a motion to dismiss, the Complaint must “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “[U]nadorned allegations of wrongdoing,” bereft of supporting facts, fall short of the “line between possibility and plausibility.” *Francis v. Giacomelli*, 588 F.3d 186, 193 (4th Cir. 2009) (citation omitted). Although the Court accepts the well-pleaded facts as true and draws all reasonable inferences in Plaintiffs’ favor, it “do[es] not blindly accept ‘allegations that

are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *Stratton v. Mecklenburg Cnty. Dep’t of Soc. Servs.*, 521 F. App’x 278, 288 (4th Cir. 2013) (quoting *Veney v. Wyche*, 293 F.3d 726, 730 (4th Cir. 2002)).

## II. Plaintiffs Fail to Allege Facts Demonstrating Article III Standing

Article III of the U.S. Constitution confines the judicial power to “Cases” and “Controversies.” *United States v. Texas*, 599 U.S. 670, 675 (2023). A case or controversy “exist[s] only if a plaintiff has standing to sue—a bedrock constitutional requirement.” *Id.* The “irreducible constitutional minimum” of standing encompasses three elements: (1) “an injury in fact,” (2) “that is fairly traceable to” the defendant’s conduct, and (3) “that is likely to be redressed by a favorable judicial decision.” *Spokeo*, 578 U.S. at 338.

“The strictures of Article III standing are no less important in the context of class actions.” *Baehr v. Creig Northrop Team, P.C.*, 953 F.3d 244, 252 (4th Cir. 2020). In a putative class action, courts “analyze standing based on the allegations of personal injury made by the named plaintiffs.” *Id.* (quoting *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613, 620 (4th Cir. 2018)).

*Injury in fact.* To establish an injury in fact at the pleading phase, a plaintiff must plausibly allege that “he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Beck*, 848 F.3d at 270 (quoting *Spokeo*, 578 U.S. at 339). That alleged injury, the Supreme Court has “emphasized repeatedly,” “must be concrete in both a qualitative and temporal sense.” *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). The injury must be “real,” not “abstract,” *Spokeo*, 578 U.S. at 340, and “distinct and palpable,” *Whitmore*, 495 U.S. at 155. “An allegation of future injury” suffices only “if the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty*

*Int'l USA*, 568 U.S. 398, 409, 414 n.5 (2013)). “Allegations of possible future injury,” or even an “objectively reasonable likelihood” of future injury, do not confer standing. *Clapper*, 568 U.S. at 409–10 (cleaned up).

*Traceability*. The plaintiff’s injury must be “fairly traceable” to the defendant’s conduct. *Spokeo*, 578 U.S. at 338. This “requirement ensures that it is likely the plaintiff’s injury was caused by the challenged conduct of the defendant, and not by the independent actions of third parties not before the court.” *Friends for Ferrell Parkway v. Stasko*, 282 F.3d 315, 324 (4th Cir. 2002). “[W]here multiple actors are involved, a plaintiff can establish causation only if the defendant’s conduct had a ‘determinative or coercive effect upon the action of someone else.’” *Alvarez v. Becerra*, No. 21-2317, 2023 WL 2908819, at \*3 (4th Cir. Apr. 12, 2023) (quoting *Bennett v. Spear*, 520 U.S. 154, 169 (1997)).

*Redressability*. It must be likely, not merely speculative, that the plaintiff’s injury will be “redressed by a favorable decision.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). Traceability and redressability “are often ‘flip sides of the same coin.’” *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 380 (2024). If the defendant caused the injury, “enjoining the action or awarding damages for the action will typically redress that injury.” *Id.* at 381. So standing generally boils down to injury in fact and causation. *Id.*

Finally, standing is not a monolith. “[P]laintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages).” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). While “a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, the risk of future harm on its own does not support Article III standing for [a] damages claim.” *Alig v. Shea*, 126 F.4th 965, 973 (4th Cir. 2025) (quoting *TransUnion*, 594 U.S. at 435,



441). Injunctive relief, in turn, requires a “showing of irreparable injury, a requirement that cannot be met where there is no showing of any real or immediate threat that the plaintiff will be wronged again.” *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1974). Without a “sufficient likelihood that [Plaintiffs] will again be wronged in a similar way, . . . past events, disconcerting as they may be, are not sufficient to confer standing to seek injunctive relief.” *Beck*, 848 F.3d at 277.

\* \* \*

The standing analysis here is simple. Plaintiffs have not alleged facts demonstrating an Article III injury. Nor is the imminent risk of future harm an injury that confers standing to pursue damages. Plaintiffs do not have standing to pursue injunctive or declaratory relief, either, because they allege no facts showing a sufficient likelihood that another data breach will occur. With no Article III standing for Plaintiffs’ claims or requested relief, this Court lacks subject-matter jurisdiction and must dismiss the Complaint.

#### **A. Plaintiffs Have Not Suffered an Article III Injury**

Plaintiffs allege a laundry list of injuries: (1) the risk of identity theft and fraud, Compl. ¶¶ 5, 23–24, 40–41, 56–57, 72, 74–75, 92–93, 108–09, 125–26; (2) loss time, productivity, and opportunity costs from mitigating the purported consequences of the data incident, *id.* ¶¶ 5, 18, 20, 23, 35, 37, 40, 51, 53, 56, 68, 70, 74, 86, 88, 92, 103, 105, 108, 120, 122, 125, 189–91, 196–98; (3) fear, anxiety, stress, annoyance, and inconvenience associated with monitoring financial accounts, *id.* ¶¶ 5, 20, 22, 37, 39, 53, 55, 70, 73, 88, 91, 105, 107, 122, 124; (4) the theft of personally identifiable information (“PII”), *id.* ¶¶ 5, 20, 37, 53, 70, 88, 105, 122; (5) the diminution of their PII value, *id.* ¶¶ 5, 20, 37, 53, 70, 88–89, 105, 122; (6) invasion of privacy, *id.* ¶¶ 5, 20–21, 37–38, 53–54, 70–71, 88, 90, 105–06, 122–23; and (7) loss of benefit of the bargain, *id.* ¶¶ 5, 20, 37, 53, 70, 88, 105, 198. None of these “harms” confers Article III standing, and most are

plainly foreclosed by binding precedent.

1. *Risk of Identity Theft and Fraud*

Plaintiffs allege that “*the risk* of identity theft is impending and has materialized,” but what follows is speculation dressed up as certainty. *See, e.g.*, Compl. ¶ 24 (emphasis added). They claim the data was “likely” published on the dark web, yet they stop short of alleging that it actually was. *Id.* They “believe” the data “was and will be sold,” not based on any facts tied to the alleged incident, but because that is supposedly what cybercriminals tend to do. *Id.*; *see also id.* ¶¶ 149, 181. This is not a factual allegation; it is a chain of hypotheticals, each resting on the last. Plaintiffs now ask the Court to treat this layered speculation as a “certainly impending” injury, despite the fact that the breach occurred nearly ten months ago and no actual misuse has been alleged since, in essence parroting legal elements but entirely neglecting the substance in support of the claims.

A threatened harm confers standing only when it is imminent, “mean[ing] that the injury is ‘*certainly* impending,’ or that there is a ‘substantial risk’ of future harm.” *Holland v. Consol Energy, Inc.*, 781 F. App’x 209, 211 (4th Cir. 2019) (quoting *Clapper*, 568 U.S. at 409). The Fourth Circuit has twice explored in depth when an increased risk of identity theft constitutes a concrete injury. *See Beck*, 848 F.3d 262 (4th Cir. 2017); *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018).

*Beck* involved two data breaches (a stolen laptop and stolen boxes of pathology reports) at a Veterans Affairs medical center. 848 F.3d at 266–68. Several veterans sued and “sought to establish Article III standing based on the harm from the increased risk of future identity theft.” *Id.* at 266–67. The Fourth Circuit noted that cases recognizing the increased risk of future identity theft as a concrete harm all involved “common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent.” *Id.* at 274. In

some, for example, “the data thief intentionally targeted the personal information compromised in the data breaches,” and in others, there were allegations of “misuse or access of that personal information by the thief.” *Id.* In *Beck*, however, the plaintiffs “ma[d]e no such claims,” “render[ing] their contention of an enhanced risk of future identity theft too speculative.” *Id.* There was no evidence or allegations of a stolen laptop or boxes of pathology reports having “been accessed or misused or that [the plaintiffs] ha[d] suffered identity theft, nor, for that matter, that the thief stole the [materials] with the intent to steal their private information.”<sup>3</sup> *Id.* at 274–75. Finding no “certainly impending” injury, the court turned to whether the plaintiffs had shown a “substantial risk” of future harm. They did not because their statistic that “33% of those affected” by the data breaches would become victims of identity theft meant that “over 66%” would not, which “falls far short of establishing a ‘substantial risk’ of harm.” *Id.* at 276.

*Hutton*, the other Fourth Circuit case that addressed when an increased risk of identity theft constitutes a concrete injury, came out the other way. In that case, “optometrists across the United States noticed that Chase Amazon Visa credit card accounts had been fraudulently opened in their names.” *Hutton*, 892 F.3d at 616. The only common link between them was the National Board of Examiners in Optometry, “where every graduating optometry student had to submit their personal information to sit for board-certifying exams.” *Id.* at 617. Unlike *Beck*, the Fourth Circuit explained, the plaintiffs “allege[d] that they ha[d] already suffered actual harm in the form of identity theft and credit card fraud. The Plaintiffs have been concretely injured by the data breach because the fraudsters used—and attempted to use—[their] information to open Chase Amazon

---

<sup>3</sup> *Beck* was a consolidated appeal, and the two underlying cases were dismissed at different procedural phases. *See Beck*, 848 F.3d at 270 (“[T]he district court dismissed *Watson* on the pleadings and *Beck* at summary judgment.”). That is why the Fourth Circuit spoke in terms of evidence and allegations (instead of only allegations). The fact that one case underwent discovery, however, played no role in the analysis. *Id.* at 275 (stating “*Watson*’s complaint suffers from the same deficiency” as the *Beck* plaintiffs’ evidence).

Visa credit card accounts.” *Id.* at 622. So there was “no need to speculate” about whether the plaintiffs would be harmed at some point in the future. *Id.*

This case bears none of the factual specificity present in *Hutton*. The sole allegation offered in support of Plaintiffs’ claim that the risk of identity theft is “impending and has materialized” is that the Plaintiffs collectively “believe” their data “was and will be sold and disseminated on the dark web,” solely because that is the “*modus operandi* of cybercriminals that commit cyberattacks of this type.” *See, e.g.,* Compl. ¶ 24 (emphasis added); *see also id.* ¶¶ 149, 181. Without any factual support or details, Plaintiffs maintain their PII was “targeted, accessed, and misused,” anchored by their speculation that there was “*likely* publication and dissemination on the dark web.” *Id.* ¶ 24 (emphasis added). But this is highly conjectural, and the Fourth Circuit has never held that the mere fact that a cybercriminal “targeted” personal information pushes a threatened injury from speculative to imminent. *See Stuart v. Kyocera AVX Components Corp.*, 769 F. Supp. 475, 485 n.5 (D.S.C. 2025) (noting that this is an open issue in the Fourth Circuit). Circuit authority appears to weigh “targeting” as a *factor* that indicates a future harm is certainly impending—not as a dispositive magic wand for standing. *See id.* (“[M]ost circuit court cases that have considered allegations of specific targeting also involved some allegations of actual misuse, whether affecting a named plaintiff or other victims, and the courts therefore did not analyze in their opinions what allegations of targeting, if any, would be sufficient to confer standing on their own.”).

Critically, “there are no allegations *of fact* [in the Complaint] sufficient to show . . . targeting.” *Podroykin v. Am. Armed Forces Mut. Aid Ass’n*, 634 F. Supp. 3d 265, 272 (E.D. Va. 2022). This case is even easier than *Podroykin*. In that case, the plaintiff alleged that a known ransomware group named DarkSide “accessed [the defendant’s] computer systems” and extracted troves of sensitive information to sell on the dark web. *Id.* at 268. Although the complaint said that

DarkSide had targeted personal information and “threatened to sell the locked data on the dark web if ransom demands [we]re not met (and they were not met in th[at] case),” the court held that “none of those allegations le[d] to the conclusion that DarkSide was targeting plaintiff’s PII, as opposed to other sensitive data.” *Id.* at 270. Here, by contrast, Plaintiffs do not allege that a cybercriminal has taken credit for the data breach and threatened to place their information on the dark web. Nor have they alleged any facts indicating that the unauthorized actor was going after *their* personal information as opposed to, say, Lafayette’s financial and business information. *See Stuart*, 769 F. Supp. at 486 (noting that the complaint alleges that the “unauthorized party obtained [PII]” but provided no allegations “lead[ing] to the conclusion that the unauthorized third party was specifically targeting Plaintiffs’ PII, as opposed to other sensitive data”).

“As the breach fades further into the past,” Plaintiffs’ “threatened injuries become more and more speculative.” *Beck*, 848 F.3d at 275 (cleaned up). It is difficult to see how identity theft and fraud could possibly be “certainly impending” for the named Plaintiffs where ten months have gone by without any indication that even a single piece of potentially compromised information from a proposed class of “approximately 75,000 persons,” Compl. ¶ 203, has been used to commit identity theft or fraud. *See Whitmore*, 495 U.S. at 158 (“A threatened injury must be certainly impending to constitute injury in fact.”). Further, “Plaintiffs’ theory of standing would still require several analytical jumps to show that fraud or identity theft was ‘certainly impending,’ including that the unauthorized third party actually sold Plaintiffs’ PII on the ‘dark web,’ that it was purchased by a bad actor, and that the bad actor has been waiting, for [ten months], to steal Plaintiffs’ identities or otherwise misuse the PII.” *Stuart*, 769 F. Supp. at 486. That is precisely the sort of “attenuated chain” that is too speculative to confer standing. *Beck*, 848 F.3d at 275.

Plaintiffs fare no better under a “substantial risk” theory. *See Driehaus*, 573 U.S. at 158

(stating a threatened harm must be “‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur” to confer standing). Their claim that personal information was “likely” published on the dark web rests on threadbare and vague assertions. Yet “[a]llegations of possible future injury,” or even an “objectively reasonable likelihood” of harm, do not suffice. *Clapper*, 568 U.S. at 409–10 (cleaned up). Indeed, in *Beck*, the plaintiffs came armed with statistics showing that “33%” of them would become victims of identity theft, and even that was not enough to show a substantial risk of harm because “over 66%” would “suffer no harm.” 848 F.3d at 276.

Finally, even if Plaintiffs had demonstrated an imminent risk of identity theft and fraud, that harm would only open the door to “forward-looking, injunctive relief to prevent the harm from occurring”—not damages. *Alig*, 126 F.4th at 973. Another shortcoming in the Complaint, however, closes the door to injunctive and declaratory relief. To enjoin a future action, a plaintiff “must demonstrate that he ‘is immediately in danger of sustaining some direct injury.’” *Beck*, 848 F.3d at 277 (quoting *Lebron v. Rumsfeld*, 670 F.3d 540, 560 (4th Cir. 2012)). This “threat of injury must be both ‘real and immediate,’ not ‘conjectural’ or ‘hypothetical.’” *Id.* Plaintiffs assert that their personal information “is subject to further unauthorized disclosures so long as [Lafayette] fails to undertake appropriate and adequate measures to protect [it].” *See, e.g.*, Compl. ¶ 88. But the fact that Plaintiffs “*could* be victimized by a future data breach . . . is not enough.” *Beck*, 848 F.3d at 277–78. Even the two data breaches in *Beck* did not show a “sufficient likelihood that [the plaintiffs would] again be wronged in a similar way.” *Id.* at 277. Plaintiffs have failed to allege facts demonstrating a “real and immediate” threat of another breach, so they do not have standing to pursue injunctive or declaratory relief. *See Lyon*, 461 U.S. at 104 (“Lyons’ assertion that he may again be subject to an illegal [act] does not create the actual controversy that must exist for a declaratory judgment to be entered.”); *Stuart*, 769 F. Supp. at 487 n.7 (“Plaintiffs’ conclusory

allegation that Defendant does not have ‘adequate safeguards’ to protect Plaintiffs’ PII, without more, is insufficient to establish standing for injunctive relief.”).

## 2. *Mitigation Efforts*

Plaintiffs next assert that they “have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach and monitoring their financial and personal accounts” and that they have “suffer[ed] actual injury in the form of lost time spent on mitigation activities.” Compl. ¶ 191.

These are precisely the kinds of boilerplate allegations that fail to establish Article III standing. Plaintiffs do not allege any actual out-of-pocket expenses, so there is no basis to conclude they suffered a concrete injury through mitigation efforts. In any event, costs “‘incurred in response to a speculative threat,’ *i.e.* their fear of future identity theft based on the breach[],” are “self-imposed harms” that do not confer standing. *See Beck*, 848 F.3d at 276-77 (quoting *Clapper*, 568 U.S. at 416); *Clapper*, 568 U.S. at 422 (“[Plaintiffs] cannot manufacture standing by incurring costs in anticipation of nonimminent harm.”); *cf. Hutton*, 892 F.3d at 622 (“[T]he [Supreme] Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm *actually exists*.” (emphasis added)). Because the risk of identity theft here is speculative, any mitigation efforts are just self-inflicted wounds.

## 3. *Emotional Harms*

Plaintiffs’ vague allegations of emotional distress resulting from the breach are foreclosed by well-established precedent. “Bare assertions of emotional injury” do not confer Article III standing. *Beck*, 848 F.3d at 273; *see also Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. SAG-22-00747, 2022 WL 3919685, at \*7 (D. Md. Aug. 31, 2022) (no concrete harm where plaintiff “merely state[d] that he has ‘sustained emotional distress’ and ‘suffered lost time,

annoyance, interference, and inconvenience . . . and has anxiety and increased concerns for the loss of his privacy,’ without alleging any facts to support these assertions”); *Podroykin*, 634 F. Supp. 3d at 272 (“[T]he *Beck* court flatly rejected the ‘claim that emotional upset and fear of identity theft and financial fraud resulting from . . . data breaches are . . . sufficient to confer Article III standing.’”). Indeed, the Supreme Court has suggested that a plaintiff would need to plead an emotional harm analogous “to the tort of intentional infliction of emotional distress” to demonstrate an Article III injury. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 n.7 (2021). Plaintiffs’ vague references to emotional distress are legally insufficient under Maryland law, which permits recovery for emotional harm only when it results in, or is accompanied by, physical injury or objective physical symptoms. *See Vance v. Vance*, 286 Md. 490, 498 (1979); *cf. Hoffman v. Stamper*, 385 Md. 1, 34–35 (2005) (recovery for emotional injury would not be allowed based on the plaintiff simply saying, “This made me feel bad; this upset me.”).

#### 4. “Theft” of PII

Each Plaintiff mentions in passing that they suffered an injury as a result of the theft of their PII. *See, e.g.*, Compl. ¶ 20. The Court can quickly dispose of this argument. Under Fourth Circuit case law, the “mere theft” or compromise of personal information does not confer standing. *See Beck*, 848 F.3d at 275 (“But the mere theft of these items [containing personal information], without more, cannot confer Article III standing.”); *see also Hutton*, 892 F.3d at 621 (“[A] mere compromise of personal information, without more, fails to satisfy the injury-in-fact element[.]”).

#### 5. Diminution of Value of Personal Information

“[C]ourts have ‘routinely rejected the proposition that an individual’s personal identifying information has an independent monetary value.’” *Podroykin*, 634 F. Supp. 3d at 272 (quoting *Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016)). Even courts that recognize this claimed



harm require “allegations of some concrete injury, such as ‘lower credit scores’ or ‘fraudulent accounts and tax returns . . . filed in [plaintiff’s] name,’” *id.* (citation omitted), or “alleg[ations] that [the] personal information actually lost value,” *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App’x 613, 614–15 (9th Cir. 2021) (“[Plaintiff] failed to adequately allege that her personal information actually lost value.”). Plaintiffs allege nothing of the sort here.

Only one named Plaintiff provides an “example” of the “diminution in the value” of his personal information, Compl.¶ 89, but the example falls flat. Plaintiff Joseph Mausteller alleges that he received a single “Lafayette Fraud Alert” notifying him of an unauthorized transaction related to Google on his Lafayette debit card nearly half a year after the security incident. *Id.* Notably, he does not allege that he was required to pay this unauthorized transaction, *see Burger v. Healthcare Mgmt. Sols., LLC*, No. RDB-23-1215, 2024 WL 473735, at \*6 (D. Md. Feb. 7, 2024) (“Burger also has not alleged that she had to pay for any of the unauthorized charges, thereby undercutting any possible injury to her”), nor does he explain how a mere fraud alert damaged the value of his personal information. Even a lowered credit score (which is not alleged by any Plaintiff here) does not confer standing unless it causes adverse financial consequences. *See, e.g., Zlotnick v. Equifax Info. Servs., LLC*, 583 F. Supp. 3d 387, 392 (E.D.N.Y. 2022) (“A lowered credit score in and of itself is not a concrete harm.”); *Basconcello v. Experian Info. Sols., Inc.*, No. 16-cv-06307-PJH, 2017 WL 1046969, at \*11 (N.D. Cal. Mar. 20, 2017) (“[A]bsent an allegation that plaintiff ‘was denied credit, lost credit, had his credit limits lowered, or was required to pay a higher interest rate for credit,’ the negative effects of a lowered credit score did not cause ‘actual’ harm.”).

More fundamentally, Plaintiffs’ theory that their personal information has lost value (and thus confers standing) simply because it was compromised would apply *in every single* data-breach case. That cannot be reconciled with the Fourth Circuit’s repeated pronouncement that the mere

fact that one's information has been compromised does not confer standing. *See Beck*, 848 F.3d at 275 (“But the mere theft of these items [containing personal information], without more, cannot confer Article III standing.”); *Hutton*, 892 F.3d at 621 (“[A] mere compromise of personal information, without more, fails to satisfy the injury-in-fact element[.]”).

#### 6. *Invasion of Privacy*

Plaintiffs' theory of “invasion of privacy” is difficult to pin down, as the Complaint consists almost entirely of legal conclusions with no well-pleaded facts to support them. To the extent they suggest that their privacy has been invaded simply because a breach occurred, that argument flies in the face of binding case law, which (again) requires something more than the “mere compromise of personal information” to “satisfy the injury-in-fact element.” *Id.*

Nor is an uptick in “spam calls and text messages” an Article III injury, *see, e.g.*, Compl. ¶ 21, let alone traceable to Lafayette. Consistent with broader deficiencies in the Complaint, Plaintiffs do not allege any specific facts to support their assertion that they experienced an increase in spam calls and texts. The Complaint does not indicate how many calls or texts were received, when they occurred, who sent them, or what they said. Without such information, these allegations are too vague and conclusory to establish an injury in fact. *See Beck*, 848 F.3d at 270 (stating in the context of a standing analysis, “we accept as true [the] allegations for which there is sufficient ‘factual matter’ to render them ‘plausible on [their] face’” (citation omitted)); *Stuart*, 769 F. Supp. at 489 (“Plaintiffs provide no factual support—including the dates or substance of the alleged calls or emails—to sufficiently allege an injury in fact.”). Further, multiple courts have observed that allegations of an uptick in spam generally only confer standing when coupled with allegations of actual misuse. *E.g., Bednyak v. Fin. Risk Mitigation, Inc.*, 739 F. Supp. 3d 353, 369–70 (E.D. La. 2024) (observing that “in every case [plaintiff] cites that post-dates *TransUnion*, each

of them involved actual misuse of the plaintiff’s PII in addition to an increase in spam calls”); *Stuart*, 769 F. Supp. at 489 n.9 (“Plaintiffs cite to several cases holding that receipt of spam constitutes an injury for the purpose of establishing standing. However, nearly all the cited cases involve allegations of actual misuse or concrete injury.”).

Even setting aside whether spam calls and texts qualify as a cognizable injury, Plaintiffs’ theory of causation is entirely speculative. Simply put, they do not allege that the data breach involved the compromise of their phone numbers. Instead, Plaintiffs rely on the theory that cybercriminals *may* have used the compromised information to locate their phone numbers through publicly available sources. Compl. ¶¶ 186–87. This theory hinges on the independent action of a third party outside of Lafayette’s control, shattering the causal chain. *See Disability Rights S.C. v. McMaster*, 24 F.4th 893, 901 (4th Cir. 2022) (“[T]he plaintiff must be able to demonstrate that the alleged harm was caused by the defendant, as opposed to the ‘independent action of some third party not before the court.’” (citation omitted)); *Clapper*, 568 U.S. at 414 (noting the Supreme Court’s “usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors”).<sup>4</sup>

Plaintiffs have failed to link the increased spam to the data breach, so any alleged injury cannot be traced back to Lafayette. *See Burger*, 2024 WL 473735, at \*6 (“[T]he generic allegation of increased spam calls and emails, if an injury at all, fails ‘to plausibly show that their alleged injuries were the result of Defendant’s conduct.’ This is especially true given that Burger has not alleged that her email address was compromised as part of the Data Breach.”); *In re Sci.*

---

<sup>4</sup> Relatedly, Plaintiff Joseph Mausteller appears to suggest, in alleging an unauthorized transaction on his Lafayette debit card, that an independent actor somehow discovered his debit card information through publicly available sources. Compl.¶ 89. Nowhere in the Complaint does he allege that the breach itself compromised this information, and even he concedes that the loss associated with “credit card theft” can be staunch immediately by closing the account, which is what he purportedly did. *Id.* ¶ 152.

*Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31 (D.D.C. 2014) (allegations that “unauthorized charges were made to [plaintiff’s] existing credit cards or debit cards, or that money was withdrawn from an existing bank account,” could not be traced to the data breach because plaintiff did not “allege[] that credit card, debit-card, or bank-account information was on the stolen tapes”).

Finally, Plaintiff Carl Lewis alleges that a password manager notified him that seven of his accounts had compromised passwords and speculates, “[u]pon information and belief,” that the Lafayette breach was the cause. Compl. ¶ 72. The Complaint, however, is devoid of any detail about what passwords or accounts were at issue, when the password manager was purchased, when the compromise occurred, whether any of the credentials were ever stored or collected by Lafayette, and what plausible harm came from these alleged compromises. There is also no allegation that any of the accounts were accessed, misused, or even targeted. Compromised passwords, standing alone, are not a concrete injury—they reflect only that credentials may have been exposed, not that any harm occurred. *See Beck*, 848 F.3d at 275 (“But the mere theft of these items [containing personal information], without more, cannot confer Article III standing.”); *Hutton*, 892 F.3d at 621 (“[A] mere compromise of personal information, without more, fails to satisfy the injury-in-fact element[.]”).

#### 7. *Loss of Benefit of the Bargain*

Plaintiffs contend that they and other consumers “understood and expected” that part of the price they paid for Lafayette’s services went toward “necessary data security” to protect their personal information. Compl. ¶ 198. But this assertion is entirely conclusory. Plaintiffs allege no facts showing that data security was a term of their agreement with Lafayette, or that any portion of the fees they paid was tied to specific data protection measures. Nor do they allege that the value

of the services they received was diminished in any measurable way as a result of the data breach. *See Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (rejecting “lost benefit of the bargain” theory where plaintiffs failed to allege “that the value of the goods or services they purchased was diminished as a result of the data breach”) (internal quotation marks and citations omitted). As a consequence, this purported harm cannot support standing.

### **B. Plaintiffs Fail to Allege an Injury Traceable to Lafayette**

Plaintiffs have not plausibly alleged that any of their claimed injuries are fairly traceable to Lafayette’s conduct. In the data breach context, Plaintiffs must come forward with “allegations demonstrating that it is both plausible and likely that [the] breach of the [defendant]’s database resulted” in the alleged harms. *Hutton*, 892 F.3d at 623. “[N]aked assertions devoid of further factual enhancement” are insufficient. *Id.* (quoting *Ashcroft*, 556 U.S at 678).

Plaintiffs acknowledge that cyberattacks are widespread across industry sectors and have occurred repeatedly in the recent past. Compl. ¶¶ 134, 136 (recognizing that “data breaches in the banking industry are becoming exponentially more common”), 144. They also acknowledge that information about them, including phone numbers, email addresses, and credit card numbers, can be considered “unregulated data” that is available through other sources and operate outside the bounds of traditional data privacy safeguards. *Id.* ¶¶ 187–88. This makes it impossible to determine whether any particular piece of allegedly misused information originated from the Lafayette breach, from a different breach, or public repository of unregulated data. *See id.* (discussing “Fullz” packages created independently by cyber-criminals and then “sold—and then resold in perpetuity—to crooked operators and other criminals”). So it is sheer speculation to suggest that the data breach at Lafayette is the source of any personal information that cybercriminals may later misuse, as opposed to publicly available information (*e.g.*, the “Fullz” packages or

“comprehensive dossier”) or even a different data breach.

This stands in sharp contrast to *Hutton*. “Notably, the Plaintiffs allege[d] that . . . [the defendant] is the *only common source* that collected and continued to store social security numbers . . . and also stored outdated personal information (such as maiden names and former married names) during the relevant time periods” and that all other potential sources “do not gather or store Social Security numbers, or have investigated and confirmed that their databases have not been breached.” *Hutton*, 892 F.3d at 623 (emphasis added). This was “sufficient factual matter,” the Fourth Circuit held, “to render the Plaintiffs’ allegations plausible on their face with respect to traceability.” *Id.* at 624. There is no “factual matter” even remotely similar to what was deemed sufficient in *Hutton* to link the data breach at Lafayette to any of Plaintiffs’ alleged harms.

The only allegations in the Complaint that arguably suggest misuse are Plaintiff Lewis’s report of compromised passwords and Plaintiff Mausteller’s receipt of a fraud alert from his bank. Compl. ¶¶ 72, 89. But the Complaint offers no factual allegations linking either event to the Lafayette breach. Plaintiffs do not allege that any specific data elements tied to those incidents—such as login credentials or credit card numbers—were compromised, nor do they provide any plausible basis to trace the alleged misuse back to Lafayette. Instead, Plaintiffs rely on a speculative theory that a cybercriminal may have obtained some unidentified piece of compromised information—possibly from this breach, possibly from another—and combined it with publicly available data to assemble a “Fullz” package that was then sold or passed on to another bad actor. *Id.* ¶¶ 183–88. This kind of attenuated, multi-step causal chain is precisely the type of conjecture the Fourth Circuit rejected in *Beck*. 848 F.3d at 275. When combined with the absence of any concrete injury—aside from a vague reference to compromised passwords and a single unauthorized charge of unknown origin—it is clear that Plaintiffs’ claims of misuse are not

plausibly traceable to the conduct of Lafayette. *See Burger*, 2024 WL 473735, at \*6 (dismissing claims for lack of standing where plaintiffs’ alleged misuse, including unauthorized charges, failed to plausibly connect any incident to the data breach or allege disclosure of any information relevant to the alleged injury).

### **C. California Plaintiffs Darbinyan and Lewis Lack UCL Standing**

Neither California Plaintiff has standing to pursue a UCL claim. To establish standing under the UCL, a plaintiff must establish that she “(1) suffered an injury in fact and (2) lost money or property as a result of the unfair competition.” *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009) (citations omitted). “A plaintiff’s personal information does not constitute property under the UCL.” *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (citation omitted), *aff’d*, 572 F. App’x 494 (9th Cir. 2014). Nor does time spent monitoring and repairing one’s credit after a breach occurs. *See Ruiz v. Gap Inc.*, No. 07-5739 SC, 2009 WL 250481, at \*3–4 (N.D. Cal. Feb. 3, 2009), *aff’d*, 380 F. App’x 689 (9th Cir. 2010). While “payments toward enhanced credit monitoring that arise from a data breach and that are not reimbursed do constitute economic injury, sufficient to confer UCL standing,” *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 661 (N.D. Cal. 2020) (quotation marks and citations omitted), the Complaint contains no such allegation. Instead, it offers only vague, boilerplate references to “lost money” and “expenses,” without identifying a single dollar spent—by any Plaintiff, let alone the California Plaintiffs—on credit monitoring or fraud mitigation. This is plainly insufficient to establish the requisite economic injury under the UCL.

### **III. Plaintiffs Fail to State a Claim**

Plaintiffs assert eight (8) claims against Lafayette: (1) negligence, (2) breach of implied contract, (3) unjust enrichment, (4) negligence *per se*, (5) breach of fiduciary duty, (6) invasion of

privacy, (7) violation of the UCL, and (8) violation of the CCPA. None of them can withstand Lafayette’s motion to dismiss.<sup>5</sup>

**A. Plaintiffs’ Negligence (Count I) and Negligence *Per Se* (Count IV) Claims Should Be Dismissed**

Plaintiffs’ Count IV—seeking damages for negligence *per se*—can be snuffed out immediately. Maryland law does not recognize negligence *per se* as an actionable claim that is separate from negligence. “[T]he settled rule in Maryland is that a statutory violation . . . does not constitute negligence *per se*, unless a statute expressly makes it so.” *Absolon v. Dollahite*, 376 Md. 547, 557 (2003); *see also In re Sabin Oral Polio Vaccine Prod. Liab. Litig.*, 774 F. Supp. 952, 956 (D. Md. 1991) (“A long line of cases holds that the doctrine of negligence *per se* has not been adopted in Maryland and that violation of a statute is merely evidence of negligence.”) (citations omitted), *aff’d*, 984 F.2d 124 (4th Cir. 1993); *Paul v. Blackburn Ltd. P’ship*, 211 Md. App. 52, 91, (2013) (“Notably, while the majority of state courts treat the statutory violation as negligence *per se*, Maryland is among the minority of states that treat the violation simply as evidence of negligence.”) (cleaned up) (internal quotation marks and citation omitted), *aff’d*, 438 Md. 100 (2014).

Here, Count IV rests solely on a purported violation of the Federal Trade Commission Act (the “**FTC Act**”) and the Gramm-Leach-Bliley Act (“**GLBA**”), asserting in conclusory terms that Lafayette failed to implement reasonable data security measures. Compl. ¶¶ 248–259; *see id.* ¶¶ 164–75. Since the FTC Act does not expressly provide that a violation of its provisions constitutes

---

<sup>5</sup> Because this is an action based on diversity, relevant state law controls. *Erie R.R. v. Tompkins*, 304 U.S. 64, 78 (1938). Here, Maryland law applies to the first six causes of action because Maryland follows the principles of both *lex loci delicti* for tort actions—applying the substantive law of the state where the alleged wrong occurred—and *lex loci contractus* for contract claims—applying the law of the jurisdiction where the contract was made. *Erie Ins. Exch. v. Heffernan*, 399 Md. 598, 618, 620 (2007). There is no dispute that the location of those purported wrongs occurred in Maryland.



negligence *per se*, Plaintiffs’ claim plainly fails. *In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2879, 2020 WL 6290670, at \*21 (D. Md. Oct. 27, 2020) (dismissing negligence *per se* claim based upon the FTC Act because applicable state law does not recognize negligence *per se* as a separate cause of action from negligence). Furthermore, the FTC Act does not provide a private right of action. *J.R. v. Walgreens Boots All., Inc.*, No. 20-1767, 2021 WL 4859603, at \*8 (4th Cir. Oct. 19, 2021). Nor does the GLBA. *Harper v. Trans Union, LLC*, No. DKC 24-230, 2025 WL 1928021, at \*5 (D. Md. July 14, 2025) (citations omitted).

Turning to Count I, Plaintiffs’ negligence claim likewise fails because there is no duty of care to support a negligence claim. *Patton v. U.S. of Am. Rugby Football*, 381 Md. 627, 636 (2004) (citation omitted). Whether a duty of care exists is a pure question of law that this Court can address immediately. *Id.*

Plaintiffs allege that Lafayette owed them a duty to safeguard their personal information and to promptly notify them in the event of a breach. Compl. ¶¶ 210–14. They claim that Lafayette breached this duty by failing to exercise reasonable care and by violating various federal statutes, including the FTC Act and GLBA. *Id.* ¶¶ 215–24. But to prevail on a negligence claim, Plaintiffs must establish “(1) that the defendant was under a duty to protect plaintiff from injury, (2) that the defendant breached that duty, (3) that the plaintiff suffered actual injury or loss, and (4) that the loss or injury proximately resulted from the defendant’s breach of the duty.” *Lloyd v. Gen. Motors Corp.*, 397 Md. 108, 131–32 (2007). Putting aside that the Plaintiffs cannot allege an injury traceable to Lafayette, neither can they establish a duty owed by Lafayette that it breached. Here, there is no duty of care because no special relationship exists between the parties: there is no contractual privity, no statutory support, no implied relationship, and nothing to implicate a duty based on the actions of a third party.

1. *Lafayette Owed No Duty of Care Because There is No Contractual Privity*

“In determining whether a tort duty should be recognized in a particular context, two major considerations are: the nature of the harm likely to result from a failure to exercise due care, and the relationship that exists between the parties.” *Jones v. Specialized Loan Servicing*, No. RDB-22-1987, 2023 WL 1442435, at \*7 (D. Md. Feb. 1, 2023) (quotation marks and citation omitted). “Where the injury is economic in nature, courts require an *intimate nexus between the parties* ‘as a condition to the imposition of tort liability.’” *Id.* (emphasis added) (quotation marks and citation omitted). “The intimate nexus is satisfied by contractual privity or its equivalent.” *Jacques v. 1st Nat’l Bank*, 307 Md. 527, 534–35 (1986).

In this case, the alleged harm is economic in nature as the alleged injuries are to neither Plaintiffs’ person nor their tangible property. *Exxon Shipping Co. v. Baker*, 554 U.S. 471, 508 n.21 (2008) (“The common law traditionally did not compensate purely economic harms, unaccompanied by injury to person or property.”) (citation omitted). Accordingly, the intimate nexus test applies, which, again, requires contractual privity or its equivalent. *Jones*, 2023 WL 1442435, at \*7. For the reasons discussed more in-depth in § III(B), there is no contractual privity (or its equivalent) between Plaintiffs and Lafayette, foreclosing the possibility that Lafayette has a tort duty as a matter of law. *See id.* (“Where there is no express or implied contract, ‘no tort duty could arise as a matter of law.’”) (quoting *Spaulding v. Wells Fargo Bank, N.A.*, 714 F.3d 769, 778 (4th Cir. 2013)).

2. *There is No Evidence of Negligence Based on Statutory Violation*

Since Maryland courts do not recognize negligence *per se* as an independent cause of action, they apply the Statute or Ordinance Rule as a means to determine whether a statutory violation can serve as *prima facie* evidence of negligence. *See Kiriakos v. Phillips*, 448 Md. 440,

457 (2016) (“The Statute or Ordinance Rule is not a means to establishing negligence per se but only prima facie evidence of negligence.”). Under Maryland’s Statute or Ordinance Rule, a plaintiff must establish both (1) a violation of a statute or ordinance intended to protect a specific class of persons, and (2) that the violation proximately caused the alleged injury. *Id.*

Plaintiffs’ allegations hold no water. They make no attempt to address the specific class of persons meant to be protected by the FTC Act or GLBA. *See Kiriakos*, 448 Md. at 457–62. The onus is on Plaintiffs to identify *specific language* in these statutes that “set forth mandatory acts clearly for the protection of a *particular class* of persons rather than the public as a whole.” *Ashburn v. Anne Arundel Cnty.*, 306 Md. 617, 635 (1986) (quotation marks and citation omitted; emphasis in original). Generally citing to the statutes without identifying this explicit language is fatal for the Plaintiffs: “Absent from these statutes and regulations is any specific mention of a duty placed upon” the alleged protected class. *Remsburg v. Montgomery*, 376 Md. 568, 585 (2003).

Indeed, Maryland courts tend to dismiss negligence claims based on statutes that have no private right of action. *See, e.g., Burger*, 2024 WL 473735, at \*8 (“Burger argues that two statutes substantiate her negligence claim: the FTC Act and the [HIPPA] . . . . However, neither statute provides a private right of action . . . undermining Burger’s special relationship theory.”) (internal citations omitted). As noted, neither the FTC Act nor the GLBA contains a private right of action. To put it simply, neither statute establishes the special relationship between Plaintiffs and Lafayette to support a negligence claim.

### 3. *There is No Duty of Care Based on an Indirect Special Relationship*

Recognizing that there is no special relationship based on contractual privity or statute, Plaintiffs maintain that a special relationship surely exists under Maryland common law because they relied upon Lafayette to safeguard their personal information. Compl. ¶ 220. This, they appear

to suggest, implies an indirect special relationship. This is fantasy. “A duty based on an implied or indirect special relationship may arise out of either: ‘(1) the inherent nature of the relationship between the parties; or (2) by one party undertaking to protect or assist the other party, and thus often inducing reliance upon the conduct of the acting party.’” *Mitchell v. WSG Bay Hills IV, LLC*, No. RDB–12–2036, 2013 WL 6502875, at \*4 (D. Md. Dec. 11, 2013) (quoting *Remsburg*, 376 Md. at 589–90). The relationship between Lafayette and Plaintiff—namely, that of a financial institution and account holder—is not the type of relationship that Maryland courts recognize as giving rise to a special duty. *See Burger*, 2024 WL 473735, at \*7 (finding no special relationship where Plaintiff’s allegations did not plausibly establish that defendant was retained for the express purpose of protecting data). Indeed, Maryland courts are “careful not to expand” a class of special relationships for fear of imposing “broad liability.” *Patton*, 381 Md. at 640 (internal quotation marks and citation omitted).

Unlike the circumstances in *In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2879, 2020 WL 6290670 (D. Md. Oct. 27, 2020), Plaintiffs do not allege that Lafayette has any contractual obligation to protect sensitive data. Rather, they allege Lafayette’s obligations to “best practices and industry standards concerning the security” of sensitive information and a privacy policy. Compl. ¶¶ 6, 143–46. Notably, there is no cause of action for a breach of an explicit contract, precisely because there are no allegations to support the claim that Lafayette was contractually hired as a data security contractor for the specific purpose of protecting any information, nor did it expressly assume such a duty. Rather, as Plaintiffs readily admit, Lafayette obtained Plaintiffs’ information in the ordinary course of offering *financial* services, not data-protection services. *See, e.g., id.* ¶¶ 13, 28.

In *Marriott*, the court allowed negligence claims to proceed based on specific allegations

that the defendant Accenture was contractually obligated to protect the plaintiffs' data and had expressly acknowledged that duty. 2020 WL 6290670, at \*7. The court emphasized that Accenture's contract with Marriott "explicitly acknowledged" an obligation to protect personal information using a reasonable standard of care, and that Accenture had publicly recognized its exposure to liability if data was improperly accessed. *Id.* No such facts are alleged here. Instead, Plaintiffs reference "best practices and industry standards" and generic statements from Lafayette's privacy policy and assert in conclusory fashion that Lafayette "knew or should have known" that Plaintiffs were relying on it to safeguard their information because financial institutions are often targets for cyberattacks. *See* Compl. ¶¶ 6, 143–46. But allegations of industry-wide risk and boilerplate privacy language fall far short of the kind of specific undertaking or mutual reliance that supported the duty finding in *Marriott*. *See also Burger*, 2024 WL 473735, at \*8.

#### 4. *No Duty Exists Based on the Actions of a Third Party*

To the extent Plaintiffs contend that Lafayette owes a duty of care because of the actions of the third-party cybercriminals, Maryland law says otherwise. Courts have consistently held that there is no duty to control the conduct of a third party to prevent harm to another absent a recognized "special relationship" either (a) between the actor and the third party, or (b) between the actor and the person injured. *Warr v. JMGM Grp., LLC*, 433 Md. 170, 185–87 (2013) (citation omitted). Maryland does not impose liability for harm caused by third parties unless the defendant had a legal duty to prevent it—regardless of whether the defendant played an active role in creating the risk or simply failed to prevent it. *Id.* at 185 n.11. The "special relationship" exception to the general rule against third-party liability is narrowly construed, *Chang-Williams v. Dep't of the Navy*, 766 F. Supp. 2d 604, 620 (D. Md. 2011) (quotation marks and citation omitted), and may

arise only in limited circumstances, such as “(1) by statute or rule; (2) by contractual or other private relationship; or (3) indirectly or impliedly by virtue of the relationship between the tortfeasor and a third party.” *Mitchell*, 2013 WL 6502875, at \*4 (quoting *Remsburg*, 376 Md. at 583–84). Because there are no allegations, and no plausible basis to infer, that Lafayette had any relationship with the third-party actors responsible for the breach, the relevant question is whether a special relationship existed between Plaintiffs and Lafayette. However, as discussed above and in detail in § III(B) *infra*, Plaintiffs cannot establish any special relationship based on statute, contract, or implied relationship. Consequently, no duty of care exists based on the actions of a third party.

**B. Plaintiffs’ Breach of Implied Contract Claim (Count II) Should Be Dismissed**

While Maryland law recognizes implied contracts,<sup>6</sup> *Dolan v. McQuaide*, 215 Md. App. 24, 36–37 (2013), Plaintiffs’ allegations miss the mark completely. Distilled down to its simplest form, an implied contract “arises from *actions* implying *definite terms*.” *Id.* at 37 (emphasis in original). “An implied-in-fact contract is a ‘true contract’ and ‘means that the parties had a contract that can be seen in their conduct rather than in an explicit set of words.’” *Mogavero v. Silverstein*, 142 Md. App. 259, 275 (2002) (quoting *Mass Transit Admin. v. Granite Constr. Co.*, 57 Md. App. 766, 774 (1984)). Thus, like an express contract, it is “‘dependent on mutual agreement or consent, and on the intention of the parties; and a meeting of the minds is required.’” *Id.* (citation omitted).

Plaintiffs have failed to allege any facts supporting a mutual agreement or the meeting of

---

<sup>6</sup> Maryland recognizes two types of implied contracts: implied-in fact and implied-in-law. *Dolan v. McQuaide*, 215 Md. App. 24, 36–37 (2013). A contract implied-in fact is a “true contract” and “means that the parties had a contract that can be seen in their conduct rather than in an explicit set of words.” *Mass Transit Admin. v. Granite Constr. Co.*, 57 Md. App. 766, 774 (1984). An implied-in-law contract, by contrast, “is indeed no contract at all” as it is a “rule of law that requires restitution to the plaintiff of something that came into defendant’s hands but belongs to the plaintiff in some sense.” *Id.* To avoid confusion, throughout this memorandum, Lafayette uses the term “implied contract” to refer to an implied-in-fact contract and the term “unjust enrichment” to refer to an implied-in-law contract.

the minds on data security measures. “Mutual assent, which is an integral component of every contract, includes two issues: (1) intent to be bound, and (2) definiteness of terms. Failure of parties to agree on an essential term of a contract may indicate that the mutual assent required to make a contract is lacking.” *Braude v. Robb*, 255 Md. App. 383, 400 (2022). For implied contracts, mutual assent exists when the conduct of the parties demonstrates a mutual intention to contract. *Brault Graham, LLC v. Law Offices of Peter G. Angelos, P.C.*, 211 Md. App. 638, 667–68 (2013). Plaintiffs identify no conduct or statement by Lafayette that manifests an agreement to undertake specific data security obligations. The Complaint points only to Plaintiffs’ unilateral expectations and general allegations that Lafayette required PII as part of a commercial transaction. *See, e.g.*, Compl. ¶¶ 13, 28. That is not enough to establish a meeting of the minds as to data security measures. *See Dolan*, 215 Md. App. at 36–37; *accord Blackman v. Ne. Spine & Sports Med., LLC*, No. 24-7022 (ZNQ), 2025 WL 77029, at \*7 (D.N.J. Jan. 13, 2025) (a complaint “must allege some other conduct by the Defendant” beyond “requir[ing] plaintiffs to provide personal information” to show “mutual assent for [the defendant] to safeguard Plaintiff’s PII”).

Even if Plaintiffs could plausibly allege mutual assent, and they do not, the implied contract claim fails for the additional reason that they identify no definite terms that could form the basis of an enforceable agreement. Under Maryland law, an implied-in-fact contract must rest on “actions implying definite terms.” *Dolan*, 215 Md. App. at 36–37. A contract, whether express or implied, cannot be enforced if “its essential terms are vague or uncertain.” *Id.* at 31–32. Plaintiffs allege only that they “reasonably believed and expected” Lafayette’s data security practices complied with laws and industry standards, and that Lafayette would “use part of those funds to obtain adequate data security.” Compl. ¶¶ 232–33. But Plaintiffs never articulate what specific protections Lafayette allegedly agreed to provide, or how those protections were communicated

or agreed upon, nor do they allege how long this so-called contract was supposed to last. *See Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 718 (8th Cir. 2017) (“Kuhns alleges that Scottrade led him to believe it would protect PII and asserts breach of this implied contract because [it] did not take reasonable measures to protect the data. But we are left to guess how Scottrade failed to take ‘industry leading’ security measures.”). Noticeably absent from the allegations are any such specific commitments by Lafayette, only generalized expectations that Lafayette would comply with “industry standards” and “relevant laws and regulations.” *See* Compl. ¶¶ 232–33. But those broad assertions do not provide the kind of definite, mutually understood terms necessary to form an enforceable contract, nor can Plaintiffs’ subjective expectations supply the missing specificity—those expectations cannot bind Lafayette in the absence of a shared understanding.

Consideration poses yet another insurmountable obstacle. To create consideration, “‘a performance or a return promise must be bargained for.’” *Braude*, 255 Md. App. at 397 (quoting *Chernick v. Chernick*, 327 Md. 470, 479 (1992)). While Plaintiffs allege that they provided personal information and paid for services, *see* Compl. ¶¶ 231–33, they do not allege that Lafayette offered adequate data security measures in exchange for that consideration. The bargained-for exchange was for banking services, not for specific cybersecurity commitments. Plaintiffs’ payment of service fees was consideration for the financial services they received—not for a separate, implied promise of data protection. And to the extent Plaintiffs argue that Lafayette’s alleged promise was merely to comply with legal or regulatory obligations, that too cannot serve as consideration. *State Constr. Corp. v. Slone Assocs., Inc.*, 385 F. Supp. 3d 449, 466 (D. Md. 2019) (citing *Russ v. Barnes*, 23 Md. App. 691, 329 A.2d 767, 770 (1974)).

Finally, even if Plaintiffs could establish the existence of a contract implied-in-fact, their claim still fails for lack of cognizable damages. The measure of damages for a contract implied-



in-fact is “based on the amount that the parties intended as the contract price or, if that amount is unexpressed, the fair market value of the [parties’] services.” *Mogavero*, 142 Md. App. at 276. But Plaintiffs do not allege that Lafayette promised any distinct service—let alone one with a determinable market value—in exchange for their personal information. Furthermore, as explained at length in § II(A) *supra*, Plaintiffs’ alleged injuries are speculative and untethered to reality. In fact, they allege no cognizable pecuniary or economic loss, which is fatal to their breach of implied contract claim. *See Adcor Indus., Inc. v. Beretta U.S.A. Corp.*, 250 Md. App. 135, 154 (2021) (“Losses that are speculative, hypothetical, remote, or contingent either in eventuality or amount will not qualify as ‘reasonably certain’ and therefore recoverable as contract damages.”).

### **C. Plaintiffs’ Unjust Enrichment Claim (Count III) Should Be Dismissed**

Plaintiffs allege that Lafayette was unjustly enriched because “they or other entities operating on their behalf purchased goods and services from [Lafayette] and provided [it] with their Private Information.” Compl. ¶ 240. They assert that Lafayette “profited from this” and “used Plaintiffs’ and the Class members’ Private Information for business purposes.” *Id.* ¶ 241. But Plaintiffs never clarify what “this” refers to, whether it means the payment for services, the provision of personal information, or some other unspecified advantage. That ambiguity underscores a more fundamental problem: Plaintiffs never identify a concrete benefit that Lafayette actually received, let alone retained unjustly.

In Maryland, a “cause of action for unjust enrichment consists of three elements: “(1) [a] benefit conferred upon the defendant by the plaintiff; (2) [a]n appreciation or knowledge by the defendant of the benefit; and (3) [t]he acceptance or retention by the defendant of the benefit under such circumstances as to make it inequitable for the defendant to retain the benefit without the payment of its value.” *Eastland Food Corp. v. Mekhaya*, 486 Md. 1, 40 (2023) (citing *Berry &*

*Gould, P.A. v. Berry*, 360 Md. 142, 151 (2000)).

Plaintiffs’ claim fails at the very first step because they do not plausibly allege that they conferred a benefit on Lafayette beyond the ordinary exchange of money for banking services. Maryland courts have made clear that unjust enrichment requires more than a generalized benefit conferred in the context of a commercial relationship. It requires a direct transfer of money or property that the defendant unjustly retains. *See Jackson v. 2109 Brandywine, LLC*, 180 Md. App. 535, 574 (2008) (“A person confers a benefit upon another if he gives to the other possession of or some other interest in money.”); *Bank of Am. Corp. v. Gibbons*, 173 Md. App. 261, 268 (2007) (“In an action for unjust enrichment the burden is on the plaintiff to establish that the defendant holds plaintiff’s money and that it would be unconscionable for him to retain it.”). Because Plaintiffs allege nothing more than a standard commercial transaction—money paid in exchange for services—they do not, and cannot, plausibly allege that Lafayette retained any benefit to which it was not entitled. Hard stop.

To the extent that their argument implies that PII is inherently valuable and thus constitutes an additional benefit conferred, Plaintiffs are mistaken. Courts across the country routinely reject the argument that PII, standing alone, has independent monetary value. *See In re Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (collecting cases). Value instead turns on how a business uses that information, such as monetizing or selling it. *See, e.g., Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 782 (S.D. Ohio 2024) (“Plaintiffs do not explain how Limestone benefited from Plaintiffs’ PII. For example, Plaintiffs do not allege that Limestone used or sold PII for a profit.”); *In re NCB Mgmt. Servs., Inc. Data Breach Litig.*, 748 F. Supp. 3d 262, 278 (E.D. Pa. 2024) (“Courts have found PII valuable to a business that commoditizes it or receives an independent pecuniary benefit from holding the PII.”).

Here, Plaintiffs offer no allegations that Lafayette monetized or otherwise derived economic value from their personal information. Nor do they allege that Lafayette should have reasonably expected to compensate Plaintiffs for that information or that Plaintiffs paid specifically for data security that was promised and not delivered. *See Harvey v. Nat'l Amusements, Inc.*, No. 24-10027-GAO, 2025 WL 928776, at \*4 (D. Mass. Mar. 17, 2025) (dismissing unjust enrichment claim where “plaintiffs d[id] not allege that [defendant] gained any benefit from storing the PII”); *Lugo v. Inova Health Care Servs.*, No. 1:24-cv-700 (PTG/WEF), 2025 WL 905191, at \*5 (E.D. Va. Mar. 25, 2025) (dismissing unjust enrichment claim where plaintiffs failed to show defendant “should have reasonably expected to pay Plaintiff[s] for [their] information that was allegedly disclosed”); *Webb v. Injured Workers Pharmacy, LLC*, No. 22-CV-10797, 2023 WL 5938606, at \*4 (D. Mass. Sept. 12, 2023) (dismissing unjust enrichment claim where plaintiffs failed to demonstrate that they “paid extra for a security package that they were promised and did not receive”).

#### **D. Plaintiffs’ Breach of Fiduciary Duty Claim (Count V) Should Be Dismissed**

To plead a breach of fiduciary duty under Maryland law, Plaintiffs must allege: (1) the existence of a fiduciary relationship; (2) a breach of the duty owed by the fiduciary to the beneficiary; and (3) resulting harm. *Plank v. Cherneski*, 469 Md. 548, 599 (2020); *Froelich v. Erickson*, 96 F. Supp. 2d 507, 526 (D. Md. 2000) (citing *Lyon v. Campbell*, 120 Md. App. 412, 439 (1998)). Plaintiffs cannot meet the first element because they fail to allege any facts establishing the existence of a fiduciary relationship between Lafayette and its customers. “Banks typically do not have a fiduciary duty to their customers.” *Spaulding*, 714 F.3d at 778.

Maryland law is cautious in creating fiduciary obligations between banks and borrowers, absent special circumstances. *Parker v. Columbia Bank*, 91 Md. App. 346, 369 (1992) (citing

*Yousef v. Trustbank Sav., F.S.B.*, 81 Md. App. 527, 536 (1990)) (“the relationship of a bank to its customer . . . is ordinarily a contractual relationship between a debtor and a creditor, and is not fiduciary in nature”); *cf. Kuechler v. Peoples Bank*, 602 F. Supp. 2d 625, 633–34 (D. Md. 2009) (applying Maryland law). *Parker* recognized four limited scenarios where special circumstances might give rise to a fiduciary duty: (1) the bank took on extra services beyond furnishing money; (2) the bank received a greater economic benefit from the transaction than normal; (3) the bank exercised extensive control; or (4) the borrower asked about liens or title. *See* 91 Md. App. at 370–71; *cf. Polek v. J.P. Morgan Chase Bank, N.A.*, 424 Md. 333, 366 (2012).

Plaintiffs allege none of these special circumstances. Instead, they assert only that they provided Lafayette with personal information in the course of obtaining services and that Lafayette stated in its privacy policy that it was committed to safeguarding that information. *See* Compl. ¶¶ 261–63. That falls flat. Courts have repeatedly found that the assertion of general privacy commitments in a public-facing policy does not create a fiduciary relationship. *See, e.g., Giasson v. MRA - Mgmt. Ass’n, Inc.*, No. 24-CV-839-JPS-JPS, 2025 WL 1025173, at \*18 (E.D. Wis. Apr. 7, 2025) (dismissing fiduciary duty claim arising from alleged mishandling of personal information where the plaintiff relied solely on general privacy statements in a company policy and failed to allege any special relationship beyond a routine commercial transaction); *Cravens v. Garda CL Se., Inc.*, No. 24-CV-80400-RLR, 2024 WL 5058304, at \*11 (S.D. Fla. Dec. 6, 2024) (rejecting the plaintiffs’ contention that “they had a fiduciary relationship with [the defendant] because ‘[the defendant] served as guardian of [the p]laintiffs’ ... PII/PHI,’ and [the defendant] became a fiduciary by ‘undertaking to collect and maintain that PII/PHI’”); *Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 781 (S.D. Ohio 2024) (rejecting the plaintiffs’ argument that their “banking relationship” with the defendant, the bank’s “accepting and maintaining [the] [p]laintiffs’ PII,” and

the bank’s “privacy policy statement on [its] website” sufficed to give rise to fiduciary duties); *Mgaresh v. Va. Union Univ.*, No. 3:24-cv-337-HEH, 2025 WL 641432, at \*1, \*5–6 (E.D. Va. Feb. 27, 2025) (declining to find fiduciary relationship between former student applicants and university where former student applicants submitted PII to defendant university as part of application process and defendant university agreed to safeguard the data).

#### **E. Plaintiffs’ Invasion of Privacy Claim (Count VI) Should Be Dismissed**

Plaintiffs attempt to recast Lafayette’s alleged failure to prevent a third-party cyberattack as an intentional invasion of privacy, but Maryland law forecloses such a claim. Maryland recognizes four distinct branches of tortious invasion of privacy, adopted from the categories enumerated in Restatement (Second) of Torts § 652A(2): (a) unreasonable intrusion upon the seclusion of another; (b) appropriation of name or likeness; (c) unreasonable publicity given to private life; and (d) publicity that places another in a false light. *See Bailer v. Erie Ins. Exch.*, 344 Md. 515, 525–26 (1997). Plaintiffs do not allege that Lafayette used their names or likenesses, published any private facts, or portrayed them in a false light. Their claim rests solely on a theory that Lafayette’s “reckless and negligent failure to protect Plaintiffs’ and the Class members’ PII constitutes an intentional interference with Plaintiffs’ and the Class members’ interest in solitude or seclusion.” Compl. ¶ 273.

That theory fails at the outset. Plaintiffs cannot use alleged negligence to establish a tort that requires intentional conduct. Intrusion upon seclusion, the only arguably applicable privacy theory, demands a deliberate invasion of a private domain that would be highly offensive to a reasonable person. *Bailer*, 344 Md. at 526–27 (“[intrusion upon seclusion] cannot be committed by unintended conduct amounting merely to a lack of due care”); *Mitchell v. Balt. Sun Co.*, 164 Md. App. 497, 522 (2005); *Furman v. Sheppard*, 130 Md. App. 67, 73 (2000). Yet Plaintiffs allege

only that Lafayette “recklessly and negligently” failed to prevent a third-party intrusion by maintaining inadequate cybersecurity. *See* Compl. ¶¶ 272–74. Notably, there is no allegation that Lafayette itself intruded into Plaintiffs’ private affairs or intended for the intrusion to occur. The contradiction is fatal: Plaintiffs cannot ground an intentional tort in conduct they themselves describe as negligent or reckless, and Lafayette’s action is one step removed from the purported intrusion upon seclusion. The claim must be dismissed.

**F. Plaintiffs Fail to State a Claim Under California Law**

1. *Plaintiffs Fail to Plausibly Allege that California Law Applies*

As a threshold matter, California statutes do not apply extraterritorially. *See Aton Ctr., Inc. v. CareFirst of Md., Inc.*, No. CV DKC 20-3170, 2021 WL 1856622, at \*12 (D. Md. May 10, 2021) (quoting *Fontenberry v. MV Transp., Inc.*, 984 F. Supp. 2d 1062, 1067 (E.D. Cal. 2013) (dismissing UCL claim where “purported *injury* was felt in California” but “there is no suggestion that *any* of the allegedly unlawful conduct was *committed* in California.”); *Gordon v. Zeroed-In Tech., LLC*, No. 23-3284-BAH, 2025 WL 936415, at \*17 (D. Md. Mar. 26, 2025) (dismissing CCPA claim for the same reason). “[State] statutes have no effect except within the state’s own territorial limits,” and Plaintiffs bear the burden of alleging facts establishing that California law governs. *Volvo Trademark Holding v. AIS Const. Equip. Corp.*, 416 F. Supp. 2d 404, 416 (W.D.N.C. 2006) (quoting *Chalmers v. Toyota Motor Sales, USA, Inc.*, 935 S.W.2d 258, 264 (Ark. 1996)). To invoke a state’s consumer protection statute, Plaintiffs must show that “the circumstances that relate to the disputed transaction occur[ed] primarily and substantially in” that state. *Int’l Equip. Trading v. Illumina, Inc.*, 312 F. Supp. 3d 725, 733 (N.D. Ill. 2018). Where “the liability-creating conduct occurs outside [a state], [that state’s] law generally should not govern.” *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018).

Here, the Complaint identifies Maryland as the sole locus of Lafayette’s operations and the relevant conduct at issue. *See* Compl. ¶¶ 128, 130, 134 (alleging Lafayette is headquartered in Rockville, Maryland, and operates locations in Maryland, Virginia, and the District of Columbia and that the focus of the security incident was PII that Lafayette “collected and stored”). Plaintiffs do not allege that Lafayette maintains any operations in California or that any relevant conduct occurred in or emanated from California. Rather, they appear to rely on their residence or purported damages as the basis for finding a connection with California. *See, e.g.,* Compl. ¶¶ 26–42, 59, 62. But this is insufficient to establish a California nexus under either the UCL or CCPA. *See Gordon*, 2025 WL 936415, at \*17 (declining to presume conduct occurred in California based solely on plaintiff’s residency, where plaintiff failed to allege facts establishing a sufficient nexus to the state); *Hill v. Workday, Inc.*, 773 F. Supp. 3d 779, 801–02 (N.D. Cal. 2025) (“[I]n UCL cases involving alleged misrepresentations, the focus is on defendant’s alleged conduct and whether or not the allegedly wrongful conduct occurred in and emanated from California, rather than on the plaintiff’s damages.”) (citation omitted).

## 2. *Plaintiffs Fail to State a Claim Under the UCL (Count VII)*

Putting aside that the California Plaintiffs lack standing to pursue their UCL claims, *see* § II(C) *supra*, the UCL claims are also subject to Rule 9(b)’s heightened pleading standard. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Although courts relax this standard for omission-based claims, plaintiffs must still plead the basic who, what, when, where, and how. *See Hill*, 773 F. Supp. 3d at 801–02. Plaintiffs allege no facts to meet this heightened requirement, instead parroting the elements of UCL claims and lodging threadbare recitals of Lafayette’s purported unlawful, unfair, and deceptive acts. This fails to pass muster as a matter of law. What the misrepresentations or omissions are defy comprehension, as the Complaint identifies no

particularized explanation of the date, substance, and speaker of these misrepresentations or omissions. This is yet another flaw of the Complaint, and this claim must be dismissed.

3. *Plaintiffs Fail to State a Claim Under the CCPA (Count VIII)*

Plaintiffs' CCPA claims are likewise deficient. The CCPA makes clear that it does not apply when the collection, selling, or sharing of personal information "takes place wholly outside of California." Cal. Civ. Code § 1798.145(a)(7). Again, the operative facts establish that Lafayette's alleged activities occurred entirely outside of California. Compl. ¶¶ 5, 130. Plaintiffs make no serious effort to establish the California nexus required under the CCPA. They do not allege that any sale or sharing of their information occurred in California—if it occurred at all. Nor do they specify when, where, or how their data was collected. Instead, they rely almost entirely on a California mailing address to invoke the power of California law against a Defendant headquartered 3,000 miles away with no operations, offices, or presence in the state. That is not enough. The CCPA requires more than a return address—it requires facts tying the alleged misconduct to California. Plaintiffs offer none.

Even assuming the CCPA applies—and it should not—the CCPA's private right of action is narrow: it applies only where a plaintiff plausibly alleges both that their personal information was (a) subject to unauthorized access, exfiltration, theft, or disclosure, and (b) that this occurred *because* the business failed to implement and maintain reasonable security procedures appropriate to the nature of the information. Cal. Civ. Code § 1798.150(a)(1). The Complaint doesn't come close to meeting either prong. It offers only conclusory buzzwords about "inadequate" security, with no plausible facts about what Lafayette actually did—or failed to do—and no meaningful link between the alleged breach and any specific deficiency in Lafayette's practices. Courts routinely reject such threadbare allegations. *See Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 57 (D.



Ariz. 2021) (dismissing CCPA claim for failure to allege facts about defendant's security measures); *Maag v. U.S. Bank, Nat'l Ass'n*, No. 21-0031, 2021 WL 5605278, at \*2 (S.D. Cal. Apr. 8, 2021) (same). Generalized references to industry "best practices" are likewise insufficient. *Griffey*, 562 F. Supp. 3d at 57. This claim must be dismissed.

### **CONCLUSION**

For the reasons above, Lafayette respectfully requests that the Court grant its motion and dismiss the Complaint in its entirety. There are no allegations that can salvage Plaintiffs' claims, so they should be dismissed with prejudice. *See United States ex rel. Carson v. Manor Care, Inc.*, 851 F.3d 293, 305 n.6 (4th Cir. 2017) ("[W]hen a complaint is incurable through amendment, dismissal is properly rendered with prejudice and without leave to amend.").

Dated: July 31, 2025

Respectfully submitted,

**LAFAYETTE FEDERAL CREDIT UNION**

By: /s/ James R. Billings-Kang

James R. Billings-Kang

James R. Billings-Kang  
COZEN O'CONNOR  
2001 M Street NW, Suite 500  
Washington, DC 20036  
(202) 280-6483  
F: (202) 640-5936  
[JBillings-Kang@cozen.com](mailto:JBillings-Kang@cozen.com)

Erin Bolan Hines, *pro hac vice forthcoming*  
COZEN O'CONNOR  
123 N. Wacker Drive, Suite 1800  
Chicago, IL 60606  
(312) 474-4490  
F: (312) 300-5645  
[EBolanHines@cozen.com](mailto:EBolanHines@cozen.com)

*Counsel for Lafayette Federal Credit Union*

**CERTIFICATE OF SERVICE**

I hereby certify that, on July 31, 2025, I will electronically file the foregoing **Memorandum of Law in Support of Defendant’s Motion to Dismiss Plaintiffs’ Consolidated Class Action Complaint** with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to all counsel of record.

/s/ James R. Billings-Kang  
James R. Billings-Kang